PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-230768
(43)Date of publication of application : 24.08.2001

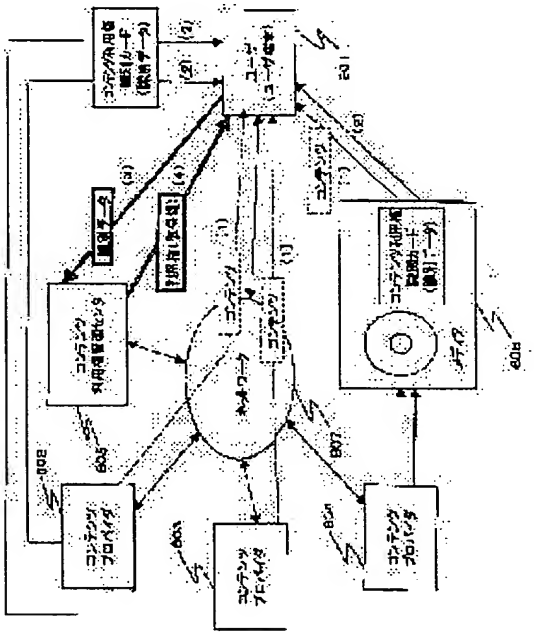
(51)Int.Cl. H04L 9/08
G06F 12/14
G06F 15/00
G06F 17/60
G07F 7/08
G07F 17/00
G09C 1/00
H04L 9/32

(21)Application number : 2000-036353
(22)Date of filing : 15.02.2000

(71)Applicant : SONY CORP
(72)Inventor : ISHIBASHI YOSHITO
SHIRAI TAIZO

(54) SYSTEM AND METHOD FOR INFORMATION TRANSACTION AND PROGRAM SUPPLY MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information transaction system and an information transaction method, which enable contents to be used without conducting a settlement by online.
SOLUTION: A contents use right identification card corresponding to ciphered contents is soled to a user. The user transmits data recorded in the content use right identification card to a contents use right management center. The contents use right management center identifies the contents and the card based on data of the received contents use right identification card, ciphers a contents key for contents decoding by a session key, for example, and transmits it to the user. The contents use right identification card sold to the user can be set so that it can be reprinted and transferred between the users. Thus, the contents key can be transmitted from the contents use right management center for plural times.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－230768
（P2001－230768A）
(43)公開日　平成13年８月24日(2001.8.24)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｅ	３Ｅ０４４
Ｇ０６Ｆ　12/14	３２０	15/00	３３０Ｚ	５Ｂ０１７
15/00	３３０	Ｇ０７Ｆ　17/00	Ｂ	５Ｂ０４９
17/60	ＺＥＣ	Ｇ０９Ｃ　1/00	６２０Ｚ	５Ｂ０８５
			６４０Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数36　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願2000－36353(P2000－36353)

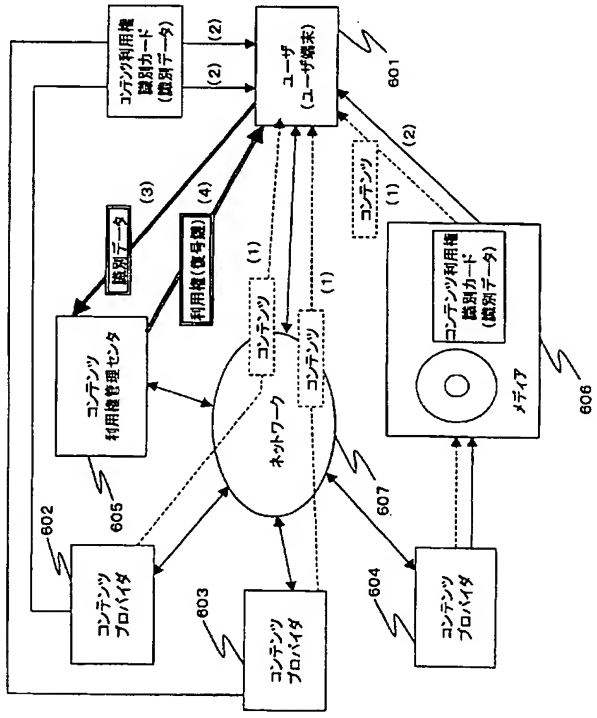
(22)出願日　平成12年２月15日(2000.2.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　白井　太三
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報取り引きシステムおよび情報取り引き方法、並びにプログラム提供媒体

(57)【要約】
【課題】　コンテンツの利用をオンラインでの決済処理を実行することなく利用可能とする情報取り引きシステムおよび情報取り引き方法を提供する。
【解決手段】　暗号化コンテンツに対応するコンテンツ利用権識別カードをユーザに販売し、ユーザはコンテンツ利用権識別カードに記録されたデータをコンテンツ利用権管理センタに送信する。コンテンツ利用権管理センタは受信したコンテンツ利用権識別カードのデータに基づいてコンテンツおよびカードを識別して、コンテンツ復号用のコンテンツ鍵をユーザに、例えばセッション鍵で暗号化して送信する。ユーザに対して販売されるコンテンツ利用権識別カードは、再販可能とする設定が可能であり、ユーザ間で譲渡することによって複数回、コンテンツ利用権管理センタからコンテンツ鍵の送信を受けることができる。



1

【特許請求の範囲】

【請求項１】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、

前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有し、

前記ユーザ機器は、通信手段または記憶媒体メディアを介して取得した暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記通信手段を介して前記コンテンツ利用権管理手段に送信する構成を有し、

前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信する構成を有することを特徴とする情報取り引きシステム。

【請求項２】前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、

前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成を有することを特徴とする請求項１に記載の情報取り引きシステム。

【請求項３】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させる構成としたことを特徴とする請求項１に記載の情報取り引きシステム。

【請求項４】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式としたことを特徴とする請求項１に記載の情報取り引きシステム。

【請求項５】前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供する構成としたことを特徴とする請求項１に記載の情報取り引きシステム。

【請求項６】前記コンテンツ利用権管理手段は、

前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、

前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、

前記コンテンツ利用権管理手段は、

前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信する構成を有することを特徴とする請求項１に記載の情報取り引きシステム。

【請求項７】前記コンテンツ利用権管理手段は、

2

同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供する構成を有し、

前記データベースには、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定した構成を有することを特徴とする請求項６に記載の情報取り引きシステム。

【請求項８】前記コンテンツ利用権識別カードは、

前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売する構成としたことを特徴とする請求項７に記載の情報取り引きシステム。

【請求項９】前記コンテンツ利用権管理手段の前記データベースは、

前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供回数を記録する構成を有することを特徴とする請求項７に記載の情報取り引きシステム。

【請求項１０】前記コンテンツ利用権管理手段の前記データベースは、

前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、

前記コンテンツ利用権管理手段は、

前記ユーザ識別データに基づいて、ユーザの利用回数をカウントする構成を有することを特徴とする請求項６に記載の情報取り引きシステム。

【請求項１１】前記コンテンツ利用権管理手段は、

前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定する構成としたことを特徴とする請求項１０に記載の情報取り引きシステム。

【請求項１２】前記コンテンツ利用権管理手段の前記データベースは、

前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、

前記コンテンツ利用権管理手段は、

前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定する構成を有することを特徴とする請求項６に記載の情報取り引きシステム。

【請求項１３】前記コンテンツ利用権識別カードは、

コンテンツ識別データ、コンテンツ利用権識別カードのカード識別データ、およびコンテンツ利用権識別カード中のデータの改竄を検証するためのチェックデータを含むことを特徴とする請求項１に記載の情報取り引きシステム。

【請求項１４】前記チェックデータは、コンテンツ利用権識別カードを発行または管理する機関による電子署名データであることを特徴とする請求項１３に記載の情報取り引きシステム。

3

【請求項１５】前記コンテンツ利用権識別カードのカード識別データは、
コンテンツ利用権識別カードの流通経路を判別可能なカード識別データであることを特徴とする請求項１３に記載の情報取り引きシステム。
【請求項１６】前記コンテンツ利用権管理手段は、
前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定する構成であることを特徴とする請求項１３に記載の情報取り引きシステム。
【請求項１７】前記コンテンツ利用権管理手段は、
前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信する構成であることを特徴とする請求項１に記載の情報取り引きシステム。
【請求項１８】前記コンテンツ利用権管理手段は、
前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信する構成であることを特徴とする請求項１に記載の情報取り引きシステム。
【請求項１９】前記コンテンツ利用権管理手段は、
前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信する構成であることを特徴とする請求項１に記載の情報取り引きシステム。
【請求項２０】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有する情報取り引きシステムにおける情報取り引き方法において、
暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、
前記コンテンツ利用権管理手段において、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信するステップと、
を有することを特徴とする情報取り引き方法。
【請求項２１】前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、
前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項２２】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させることを特徴とする請求項２０に記載の情報取り引き方法。

4

【請求項２３】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式であることを特徴とする請求項２０に記載の情報取り引き方法。
【請求項２４】前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項２５】前記コンテンツ利用権管理手段は、
前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、
前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、
前記コンテンツ利用権管理手段は、
前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項２６】前記コンテンツ利用権管理手段は、
同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供し、
前記データベースに、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定することを特徴とする請求項２５に記載の情報取り引き方法。
【請求項２７】前記コンテンツ利用権識別カードは、
前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売することを特徴とする請求項２６に記載の情報取り引き方法。
【請求項２８】前記コンテンツ利用権管理手段は、
前記データベースに、前記コンテンツ利用権識別カード毎のコンテンツ鍵の提供回数を記録することを特徴とする請求項２６に記載の情報取り引き方法。
【請求項２９】前記コンテンツ利用権管理手段の前記データベースは、
前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、
前記コンテンツ利用権管理手段は、
前記ユーザ識別データに基づいて、ユーザの利用回数をカウントすることを特徴とする請求項２５に記載の情報取り引き方法。
【請求項３０】前記コンテンツ利用権管理手段は、
前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定することを特徴とする請求項２９に記載の情報取り引き方法。

5

【請求項３１】前記コンテンツ利用権管理手段の前記データベースは、
前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、
前記コンテンツ利用権管理手段は、
前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定することを特徴とする請求項２５に記載の情報取り引き方法。
【請求項３２】前記コンテンツ利用権管理手段は、
前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項３３】前記コンテンツ利用権管理手段は、
前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項３４】前記コンテンツ利用権管理手段は、
前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項３５】前記コンテンツ利用権管理手段は、
前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信することを特徴とする請求項２０に記載の情報取り引き方法。
【請求項３６】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器におけるコンテンツ情報取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
オフラインでユーザに提供されるコンテンツ利用権識別カードに記録されたコンテンツ利用権識別データを前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、
前記コンテンツ利用権管理手段から受信したコンテンツ鍵に基づいて暗号化コンテンツを復号処理するステップと、
を有することを特徴とするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は情報取り引きシステムおよび情報取り引き方法、並びにプログラム提供媒体に関する。特に、音楽、画像データ、ゲームプログラム等の各種コンテンツ情報をＣＤ，ＤＶＤ等の記録媒体を介して、あるいはネットワークを介した配信によりユーザに提供し、ユーザからコンテンツ利用に伴う利用料金の回収あるいは利用ポイントの付与等を実行する構成を有する情報取り引きシステムおよび情報取り引き方法に関する。

6

【０００２】
【従来の技術】昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体（メディア）を介して流通している。これらの流通コンテンツは、一般にユーザの所有するＰＣ（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモリカード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。
【０００３】従来のビデオゲーム機器、ＰＣ等の情報機器において使用されるメモリカード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモリカードに備えられた不揮発性メモリはＥＥＰＲＯＭ、フラッシュメモリ等によって構成される。
【０００４】ＤＶＤ、ＣＤ等の流通可能な記憶媒体（メディア）、あるいはメモリカード等の記憶手段に記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により各記憶手段から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。
【０００５】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、コンテンツの配布時、すなわちコンテンツがＤＶＤ，ＣＤ等の記憶媒体によって流通する場合には、ＤＶＤ，ＣＤ等の記憶媒体の販売時に代金を回収したり、あるいはインターネット等のネットワークを介してコンテンツを配信する場合には、コンテンツ配信に際してユーザのクレジット番号等のユーザ情報を取得してユーザからコンテンツ提供に対する対価、すなわち利用料金を取得する構成を採用している。
【０００６】これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないよう、セキュリティを考慮した構成をとるのが一般的となっており、ＤＶＤ，ＣＤ等の記憶媒体（メディア）、あるいはネットワークを介したコンテンツデータの配信においては、配布コンテンツを暗号化して、正規

なユーザであると確認された場合にのみ、暗号化コンテンツを復号可能な鍵（コンテンツ鍵）を提供する構成が採用されている。

【０００７】例えば、昨今のデジタルデータ（コンテンツ）のオンライン販売システムの構成としては、ユーザがネットワークやメディア経由で暗号化されたコンテンツを取得し、コンテンツを利用するために、ユーザ端末をコンテンツ利用権販売センターに接続してコンテンツの利用権購入手続きをオンラインで行ない、暗号化コンテンツの復号処理に適用する鍵をネットワークを介して取得する態様が普及しつつある。

【０００８】暗号化されたコンテンツデータは、オンライン手続きによってコンテンツ利用権販売センターから取得した鍵を用いて復号化処理が可能となり、復号処理によってユーザ端末において利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００９】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Data encryption standard）がある。

【００１０】上述の暗号化処理、復号化処理に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【００１１】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が配布した公開鍵または認証局から入手した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を配布した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。

【００１２】このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図１を用いて簡単に説明する。

【００１３】図１は、ＰＣ（パーソナルコンピュータ）、ゲーム機器等の再生手段１０において、ＤＶＤ，ＣＤ３０、インターネット４０等のデータ提供手段から取得したプログラム、音声データ、映像データ等（コンテンツ（Content））を再生するとともに、ＤＶＤ，ＣＤ３０、インターネット４０等から取得したデータをフロッピーディスク、メモリカード、ハードディスク等の記憶手段２０に記憶可能とした構成例を示すものである。

【００１４】プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段１０を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。

【００１５】再生手段１０はＣＰＵ１２を有し、入力データの再生処理を再生処理部１４で実行する。再生処理部１４は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

【００１６】正規ユーザは、提供されたプログラムを、再度使用するために記憶手段２０にプログラム／データ等、コンテンツの保存処理を行なう。再生手段１０には、このコンテンツ保存処理を実行するための保存処理部１３を有する。保存処理部１３は、記憶手段２０に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。

【００１７】コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部１３は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをＦＤ（フロッピーディスク）、メモリカード、ハードディスク等の記憶手段２０の記憶部２１に記憶する。

【００１８】ユーザは、記憶手段２０から格納コンテンツを取り出して再生する場合には、記憶手段２０から、暗号化データを取り出して、再生手段１０の再生処理部１４において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

【００１９】

【発明が解決しようとする課題】このような暗号化コンテンツの利用には、前述したようにコンテンツ利用権販売センタからコンテンツの正規利用権を取得し、暗号化コンテンツの復号処理に適用する鍵を購入することが必要となるが、この購入代金の支払いの方法としては、例

えば（１）クレジットカード番号を端末から入力してコンテンツ利用権販売センタに送信する。（２）ユーザの銀行口座番号を端末から入力してコンテンツ利用権販売センタに送信する。（３）予めコンテンツ利用権販売センタにユーザ登録を行ない、クレジットカード番号、あるいは銀行口座番号を登録し、コンテンツ利用権販売センタが登録済みデータに基づいて引き落としを実行する。（４）電子マネーを利用する。これらの各種の方法がある。

【００２０】しかしながら、これら（１）～（３）の支払方法においてはユーザのクレジットカード番号、あるいは銀行口座番号が要求されることになる。従って、これらのクレジットカード、銀行口座を持たない例えば未成年者にとっては、この支払い手続きが困難になる。さらに、昨今では、取り引きコンテンツ単位が小口化し、例えば音楽コンテンツの配信において曲目１曲のみを取り引きコンテンツとすることもある。このような場合、コンテンツの代金は、１００円単位、１０００円単位の小額のものとなり、これらの支払いにおいて、逐一、クレジットカード番号、あるいは銀行口座番号が要求されるという取り引き形態は、コンテンツの流通を妨げる一因ともなっている。

【００２１】また、上述の（４）電子マネーの利用については、現状ではまだ試用段階であり、その利用形態が確立されておらず、一般に普及するには至っていないのが現状である。

【００２２】本発明は、これらの状況に鑑みてなされたものであり、ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツ利用権の販売において、クレジットカード番号、あるいは銀行口座番号、電子マネー等を利用せず、簡易な方法、構成の情報取り引きシステムおよび情報取り引き方法、並びにプログラム提供媒体を提供することを目的とする。

【００２３】

【課題を解決するための手段】本発明は、上記課題を解決するためになされたものであり、本発明の第１の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有し、前記ユーザ機器は、通信手段または記憶媒体メディアを介して取得した暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記通信手段を介して前記コンテンツ利用権管理手段に送信する構成を有し、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信する構成を有することを特徴とする情報取り引きシステムにある。

【００２４】さらに、本発明の情報取り引きシステムの一実施態様において、前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成を有することを特徴とする。

【００２５】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させる構成としたことを特徴とする。

【００２６】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式としたことを特徴とする。

【００２７】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供する構成としたことを特徴とする。

【００２８】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信する構成を有することを特徴とする。

【００２９】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供する構成を有し、前記データベースには、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定した構成を有することを特徴とする。

【００３０】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売する構成としたことを特徴とする。

【００３１】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード

毎に、コンテンツ鍵の提供回数を記録する構成を有することを特徴とする。

【００３２】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントする構成を有することを特徴とする。

【００３３】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定する構成としたことを特徴とする。

【００３４】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定する構成を有することを特徴とする。

【００３５】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、コンテンツ識別データ、コンテンツ利用権識別カードのカード識別データ、およびコンテンツ利用権識別カード中のデータの改竄を検証するためのチェックデータを含むことを特徴とする。

【００３６】さらに、本発明の情報取り引きシステムの一実施態様において、前記チェックデータは、コンテンツ利用権識別カードを発行または管理する機関による電子署名データであることを特徴とする。

【００３７】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードのカード識別データは、コンテンツ利用権識別カードの流通経路を判別可能なカード識別データであることを特徴とする。

【００３８】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定する構成であることを特徴とする。

【００３９】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信する構成であることを特徴とする。

【００４０】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信する構成であることを特徴とする。

【００４１】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信する構成であることを特徴とする。

【００４２】さらに、本発明の第2の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有する情報取り引きシステムにおける情報取り引き方法において、暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、前記コンテンツ利用権管理手段において、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信するステップと、を有することを特徴とする情報取り引き方法にある。

【００４３】さらに、本発明の情報取り引き方法の一実施態様において、前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得することを特徴とする。

【００４４】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させることを特徴とする。

【００４５】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式であることを特徴とする。

【００４６】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供することを特徴とする。

【００４７】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前

記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信することを特徴とする。

【００４８】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供し、前記データベースに、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定することを特徴とする。

【００４９】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売することを特徴とする。

【００５０】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記データベースに、前記コンテンツ利用権識別カード毎のコンテンツ鍵の提供回数を記録することを特徴とする。

【００５１】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントすることを特徴とする。

【００５２】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定することを特徴とする。

【００５３】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定することを特徴とする。

【００５４】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定することを特徴とする。

【００５５】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信することを特徴とする。

【００５６】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信することを特徴とする。

【００５７】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信することを特徴とする。

【００５８】さらに、本発明の第３の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器におけるコンテンツ情報取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、オフラインでユーザに提供されるコンテンツ利用権識別カードに記録されたコンテンツ利用権識別データを前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、前記コンテンツ利用権管理手段から受信したコンテンツ鍵に基づいて暗号化コンテンツを復号処理するステップと、を有することを特徴とするプログラム提供媒体にある。

【００５９】本発明の第３の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯ、ＤＶＤなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００６０】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００６１】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【００６２】

【実施例】図２に本発明の情報取り引きシステムに使用されるユーザ端末であるデータ処理装置の一実施例に係る構成ブロック図を示す。データ処理装置は、記録再生器３００と記録デバイス４００とを主要構成要素とする。

【００６３】記録再生器３００は、例えばパーソナル・コンピュータ（ＰＣ：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器３００は、図２に示すように、記録再生器３００における暗号処理時の記録デバイス４００との通信制御を含む統括的制御を実行する制御部３０１、暗号処理全般を司る記録再生器暗号処理部３０２、記録再生器に接続される記録デバイス４００と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ３０３、ＤＶＤなどのメディア５００から少なくともデータの読み出しを行う読み取り部３０４、外部とデータの送受信を行う通信部３０５を有する。

【００６４】記録再生器３００は、制御部３０１の制御により記録デバイス４００に対するコンテンツデータのダウンロード、記録デバイス４００からのコンテンツデータ再生を実行する。記録デバイス４００は、記録再生器３００に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、ＥＥＰＲＯＭ、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成される外部メモリ４０２を有する。

【００６５】記録再生器３００は、図２の左端に示す記憶媒体、ＤＶＤ、ＣＤ、ＦＤ、ＨＤＤに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部３０４、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部３０５を有し、外部からコンテンツを入力する。

【００６６】記録再生器３００は、暗号処理部３０２を有し、読み取り部３０４または通信部３０５を介して外部から入力されるコンテンツデータを記録デバイス４００にダウンロード処理する際、あるいはコンテンツデータを記録デバイス４００から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。暗号処理部３０２は、暗号処理部３０２全体を制御する制御部３０６、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ３０７、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部３０８から構成されている。

【００６７】制御部３０１は、例えば、記録再生器３００と通信部３０５を介して接続されたコンテンツ利用管理センタ（図３以下で説明）と暗号処理部３０２の相互認証処理における仲介制御、セッション鍵で暗号化されて送付されるコンテンツ鍵の暗号処理部３０２における復号処理における仲介制御、さらに記録デバイス４００が装着された際に記録デバイスコントローラ３０３を介して記録デバイス４００に初期化命令を送信したり、あるいは、記録再生器暗号処理部３０２の暗号／復号化部３０８と記録デバイス暗号処理部４０１の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。

【００６８】暗号処理部３０２は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部３０６、内部メモリ３０７、暗号／復号化部３０８を有する。

【００６９】暗号処理制御部３０６は、記録再生器３００において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、コンテンツ利用管理センタ（図３以下で説明）との相互認証処理、記録再生器３００と記録デバイス４００との間で実行される相互認証処理の制御、記録再生器暗号処理部３０２の暗号／復号化部３０８において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関する暗号処理の実行命令等、暗号処理全般に関する制御を行なう。

【００７０】内部メモリ３０７は、記録再生器３００において実行される相互認証処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは記録再生器の識別データ等を格納する。記録再生器の識別データは、コンテンツ利用管理センタ（図３以下で説明）との相互認証処理等において必要となる。また、後段で説明するが、コンテンツ利用管理センタのデータベース中に登録されるデータとして利用される。

【００７１】暗号／復号化部３０８は、内部メモリ３０７に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス４００にダウンロード処理する際、あるいは記録デバイス４００に格納されたコンテンツデータを記録デバイス４００から再生、実行する際の認証処理、暗号化処理、復号化処理、データの検証、乱数の発生などの処理を実行する。

【００７２】ここで、記録再生器暗号処理部３０２の内部メモリ３０７は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部３０２は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニュウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【００７３】記録再生器３００は、これらの暗号処理機能の他に、中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６、ＲＡＭ（Random Access Memory）１０７、ＲＯＭ(Read Only Memory)１０８、ＡＶ

処理部１０９、入力インタフェース１１０、ＰＩＯ（パラレルＩ／Ｏインタフェース）１１１、ＳＩＯ（シリアルＩ／Ｏインタフェース）１１２を備えている。

【００７４】中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６、ＲＡＭ（Random Access Memory）１０７、ＲＯＭ(Read Only Memory)１０８は、記録再生器３００本体の制御系として機能する構成部であり、主として記録再生器暗号処理部３０２で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインＣＰＵ：Central Processing Unit）１０６は、制御部３０１の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをＡＶ処理部１０９へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【００７５】ＲＡＭ１０７は、ＣＰＵ１０６における各種処理用の主記憶メモリとして使用され、メインＣＰＵ１０６による処理のための作業領域として使用される。ＲＯＭ１０８は、メインＣＰＵ１０６で起動されるＯＳ等を立ち上げるための基本プログラム等が格納される。

【００７６】ＡＶ処理部１０９は、具体的には、例えばＭＰＥＧ２デコーダ、ＡＴＲＡＣデコーダ、ＭＰ３デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【００７７】入力インタフェース１１０は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインＣＰＵ１０６に出力する。メインＣＰＵ１０６は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

【００７８】ＰＩＯ（パラレルＩ／Ｏインタフェース）１１１、ＳＩＯ（シリアルＩ／Ｏインタフェース）１１２は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

【００７９】また、メインＣＰＵ１０６は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス４００に記憶する際の制御も行なう。この処理の際には、記憶データを制御部３０１に転送し、制御部３０１は必要に応じて暗号処理部３０２にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス４００に格納する。

【００８０】記録デバイス４００は、好ましくは記録再生器３００に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス４００は暗号処理部４０１、外部メモリ４０２を有する。

【００８１】記録デバイス暗号処理部４０１は、記録再生器３００からのコンテンツデータのダウンロード、または記録デバイス４００から記録再生器３００へのコンテンツデータの再生処理時等における記録再生器３００と記録デバイス４００間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、記録再生器３００の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。外部メモリ４０２は、前述したように、例えばＥＥＰＲＯＭ、フラッシュメモリ等からなる不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成されコンテンツデータを格納する。

【００８２】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツを提供するコンテンツプロバイダ、あるいはコンテンツの利用権を管理するコンテンツ利用権販売センタは、提供コンテンツを暗号化して、ＣＤ，ＤＶＤ等のメディア、あるいはネットワークを介してユーザに提供する。さらに、ＣＤ，ＤＶＤ等のメディアを介してコンテンツを流通させる場合は、コンテンツ利用権を証明する識別子を記入したカード（以下、コンテンツ利用権識別カード）を外部からは観察できないように密封してメディアに同梱して販売する。コンテンツ利用権識別カードは、識別子が外部から観察できないようにメディアパッケージ内に密封しておく。例えばスクラッチカード等のような形態を採用してもよい。

【００８３】また、ネットワークを介してコンテンツを配信する場合は、コンテンツ利用権を証明する識別子を記入したカード、すなわちコンテンツ利用権識別カードは、オンラインで取り引きすることなく、オフライン、すなわち店舗等を経由してコンテンツ利用権識別カードのみをコンテンツとは別に販売する。この場合においてもコンテンツ利用権識別カードは、外部からは観察できないようにパッケージ内に密封したり、スクラッチカード等のような形態とする。

【００８４】図３に、ユーザ端末と、コンテンツプロバイダと、コンテンツ利用権管理センタ間において実行されるコンテンツと、コンテンツ利用権識別カードと、コンテンツ利用権（復号鍵として利用されるコンテンツ鍵）の流通形態を説明する図を示す。

【００８５】図３において、ユーザ（ユーザ端末）６０１は、例えば図２で説明した記録再生器である。さらに、ユーザ端末６０１は、ユーザ個人の所有するパーソナルコンピュータ、ゲーム機器、あるいは駅、コンビニ等の共同スペースに設置され不特定多数が利用可能な端末であってもよい。

【００８６】音楽、画像、ゲームプログラム等、各種コンテンツを利用したいユーザは、ユーザ端末６０１を利用して、コンテンツプロバイダ６０２，６０３，６０４から、ネットワーク６０７を介して暗号化されたコンテンツの配信を受けたり、あるいはメディア６０６を介してコンテンツを入手する。さらに、コンテンツ購入者は、コンテンツの入手に併せてコンテンツ利用権識別カ

ードを購入、受領する。

【００８７】コンテンツ利用権識別カードは、ユーザ（ユーザ端末）６０１がコンテンツの利用権を取得するための識別子が記録されたカードである。すなわち暗号化コンテンツの復号鍵を取得するために必要な識別子が記録されたカードである。このコンテンツ利用権識別カードは、暗号化コンテンツの配布ルートがＤＶＤ，ＣＤ等のメディアを介した形態である場合は、メディアに同梱する形態とし、また、ネットワークを介したコンテンツ配信の場合は、独立してコンテンツ利用権識別カードを配布、あるいは販売する。なお、メディアを介したコンテンツ配布の場合においても、コンテンツ利用権識別カードはメディアと同梱とすることなく、別個に独自の流通ルートで配布するようにしてもよい。いずれの場合も、コンテンツ利用権識別カードは、流通経路上では、外部から識別子データが観察できないように密封構成、例えばスクラッチ式のカードとして配布あるいは販売する。

【００８８】暗号化コンテンツをユーザに提供するコンテンツプロバイダ６０２，６０３，６０４は、コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成とすることで、ユーザからのオンラインによる料金徴収の取り引きを省略することができる。なお、コンテンツ利用権識別カードのユーザに対する提供に応じた対価の配分は、コンテンツプロバイダ、コンテンツ利用権管理センタ、さらにコンテンツ利用権識別カードを販売した店舗等の間で適宜配分するようにしてもよい。

【００８９】コンテンツ利用権識別カードに記録される識別データの例を図４に示す。図４に示すように、識別データには、利用対象となるコンテンツを識別するコンテンツ識別子（ＩＤ）と、シリアル番号、電子署名が記録されている。コンテンツ識別子（ＩＤ）はユーザがコンテンツプロバイダからメディアまたはネットワークを介して入手した利用予定のコンテンツを識別するデータである。シリアル番号は、コンテンツ利用権識別カード毎の番号であり、個々のコンテンツ利用権識別カードを識別可能な番号となっている。電子署名は、コンテンツの利用権を管理する例えばコンテンツ利用管理センタ６０５（図３参照）の署名鍵によって、コンテンツＩＤ、シリアル番号に対して生成された署名データであり、コンテンツＩＤ、シリアル番号の改竄を防止するために付加されている。電子署名は、コンテンツ利用権識別カードを発行または管理する機関によって行われる。なお、図４では、電子署名をコンテンツ利用権識別カードに記録されるチェックデータとして使用しているが、電子署名を用いない、例えばチェックサムのような簡易なチェックデータを付与する構成としてもよい。

【００９０】図３に戻り、ユーザ端末と、コンテンツプロバイダと、コンテンツ利用権管理センタ間において実

行されるコンテンツと、コンテンツ利用権識別カードと、コンテンツ利用権（復号鍵）の流通形態の説明を続ける。

【００９１】暗号化コンテンツをメディア６０６またはネットワーク６０７を介して受領したユーザ（ユーザ端末）６０１は、図４で説明したデータ構成を持つコンテンツ利用権識別カードをメディア６０６に併せて、あるいは別ルートで購入、受領する。

【００９２】コンテンツ利用権識別カードを購入、受領したユーザ６０１は、コンテンツ利用権識別カードに記録された、コンテンツＩＤ、シリアル番号、電子署名から構成される識別データをコンテンツ利用権管理センタ６０５にネットワーク６０７を介して送信する。

【００９３】コンテンツ利用権管理センタ６０５は、発行済みのコンテンツ利用権識別カードに関する情報をデータベースにより管理しており、例えばシリアル番号で識別されるコンテンツ利用権識別カードに対応するコンテンツの復号鍵の配布がすでに実行されているか否か等のデータを管理している。コンテンツ利用権管理センタ６０５は、ユーザから受領したコンテンツ利用権識別カードに記録された、コンテンツＩＤ、シリアル番号、電子署名から構成される識別データを正当であるかどうかを判定し、さらに、コンテンツを識別し、また、すでに鍵を配信しているかどうか等をチェックする。

【００９４】これら各種のチェックの後、コンテンツ利用権管理センタ６０５がユーザに対してコンテンツ利用権を配布すると判定した場合は、ユーザに対する復号鍵（コンテンツ鍵）の配布を行なう。なお、コンテンツ鍵の配布は、ネットワークでの通信の安全性を考慮して暗号化して送付することが望ましく、例えばユーザ端末との相互認証処理後に共有するセッション鍵で暗号化して送信する。鍵を受信したユーザは、受領した暗号化コンテンツ鍵をセッション鍵で復号して、復号したコンテンツ鍵を用いて暗号化コンテンツの復号処理を実行して、コンテンツを利用可能とする。

【００９５】コンテンツ利用管理センタ６０５が有するコンテンツ利用権識別カードに関するデータベースを図５に示す。データベースには、利用対象となるコンテンツを識別するコンテンツ識別子（ＩＤ）と、シリアル番号、利用権（復号鍵）の販売回数、利用権の購入者情報、その他の情報が含まれる。コンテンツ識別子（ＩＤ）と、シリアル番号は、前述の図４において説明したコンテンツ利用権識別カード中のデータに対応するデータである。利用権（復号鍵）の販売回数は、後段でさらに説明するが、１つのコンテンツ利用権識別カードを再販することによって、複数回、利用権を販売した場合に、その回数を記録したものである。購入者情報は、購入者の識別データを記録している。その他の情報としては、シリアル番号に対応するコンテンツ利用権識別カードの再販可能性の有無、さらに再販可能である場合の再

販可能回数が記録されている。再販については、後段で説明する。

【００９６】図５に示す例においては、コンテンツ利用権識別カードに応じて再販可能なカードであるもの（上段２つ）と、再販不可能なもの（中段２つ）と、再販可能なカードにおいて最大販売回数が規定されたもの（下段２つ）のそれぞれがデータベース中に設定されている。

【００９７】図６に本発明の情報取り引きシステムを構成する、コンテンツ利用権管理センタと、コンテンツプロバイダと、ユーザ端末の構成ブロック図を示す。ユーザ端末９００は、前述の図２で説明した記録再生器３００と同様であり、同一構成部には同一符号を付してある。記録再生器３００の各構成要素については、図２において説明したので、説明を省略する。

【００９８】図６において、コンテンツ利用権管理センタ７００は、ユーザ端末９００と通信を実行するための通信部７０３、通信制御を含む統括的制御を実行する制御部７０１、暗号処理全般を司る暗号処理部７０２、前述の図５で説明したコンテンツ利用権識別カードの管理データを格納したデータベース７０４、コンテンツの復号処理に用いるコンテンツ鍵を格納するコンテンツ鍵格納メモリ７０５を有している。暗号処理部７０２は、ユーザ端末９００との相互認証処理、セッション鍵生成処理、セッション鍵によるコンテンツ鍵の暗号化処理を実行する。

【００９９】また、コンテンツプロバイダ８００は、メディア５００、またはネットワーク等の通信手段６００を介して暗号化コンテンツをユーザに対して供給する構成を持ち、コンテンツを格納したコンテンツデータベース８０４、コンテンツの暗号処理を実行する暗号処理部８０２、ユーザ端末との通信を実行する通信部８０３、通信制御を含む統括的制御を実行する制御部８０１を有する。なお、図６に示すコンテンツプロバイダの構成は一例であり、例えばメディアのみの供給を行なうプロバイダであれば通信手段を必要としない。

【０１００】また、図６では、コンテンツ管理センタと、コンテンツプロバイダとを独立した手段として示してあるが、両機能を併せ持った１つの手段でコンテンツ管理センタとコンテンツプロバイダの両機能を提供するように構成としてもよい。

【０１０１】図６に示す構成において実行される各処理手続きの詳細について説明する。まず、図４で説明したコンテンツ利用権識別カードは、コンテンツ利用権管理センタ７００がコンテンツプロバイダ８００からのコンテンツ配布に伴って作成する。コンテンツ管理センタ７００は、新たに配布されるコンテンツにコンテンツ識別子を付与し、さらに、発行するコンテンツ利用権識別カード毎にシリアル番号を付与し、さらに、これらのコンテンツ識別子とシリアル番号に対して電子署名を生成して、図４で説明したデータを有するコンテンツ利用権識別カードを生成し、これをコンテンツプロバイダの供給するコンテンツ、例えばメディアに同梱してユーザに提供する。あるいはコンテンツプロバイダがネットワーク配信によりコンテンツを提供する場合は、コンテンツとは別ルートで、例えば特定の店舗においてコンテンツ利用権識別カードを販売、配布する。

【０１０２】なお、ここでは、コンテンツ利用権管理センタ７００がコンテンツ利用権識別カードを作成する例を説明するが、コンテンツプロバイダがコンテンツ利用権識別カードを作成して、作成したコンテンツ利用権識別カード情報をコンテンツ利用管理センタに提供し、その後の利用権配布手続きをコンテンツ利用権管理センタ７００に任せる構成としてもよい。

【０１０３】コンテンツ利用権識別カードの構成データである電子署名データの生成処理方法の例の１つとして共通鍵暗号方式におけるＤＥＳを用いた例を説明する。なお、本発明においては、ＤＥＳ以外にも、同様の共通鍵暗号方式における処理として例えばＦＥＡＬ（Fast Encipherment ALgorithm：ＮＴＴ）、ＡＥＳ（Advanced Encryption Standard：米国次期標準暗号）等を用いることも可能である。

【０１０４】一般的なＤＥＳを用いた電子署名の生成方法を図７を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを８バイト単位に分割する（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）。そして、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮが電子署名になる。この値は一般にはメッセージ認証符号（ＭＡＣ（Message Authentication Code））と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをＣＢＣ（Cipher Block Chaining）モードと呼ぶ。このＭＡＣ値の検証時には、検証者が生成時と同様の方法でＭＡＣ値を生成し、同一の値が得られた場合、検証成功とする。

【０１０５】本発明の情報取り引きシステムにおいて使用されるコンテンツ利用権識別カードには、図４を用いて説明したようにコンテンツＩＤとシリアル番号が含まれ、これらが検証対象のメッセージに対応する。従って、これらのデータ、あるいはこれらのデータに基づいて生成されるデータを図７に示すＤＥＳ暗号処理部に入力するメッセージとして電子署名を生成する。

【０１０６】次に、公開鍵暗号方式を用いた電子署名の

23

生成方法を図８を用いて説明する。図８に示す処理は、ＥＣ－ＤＳＡ（(Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（(Rivest、Shamir、Adleman)など（ANSI X9.31））を用いることも可能である。

【０１０７】図８の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【０１０８】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【０１０９】続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【０１１０】

【数１】P=(Xa, Ya), Q=(Xb, Yb), R=(Xc, Yc)=P+Qとすると、P≠Qの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Qの時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【０１１１】これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する$2^i\times G$（Ｇをｉ回２倍算した値）を加算する（ｉはｕのＬＳＢから数えた時のビット位置））。

【０１１２】ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

24

【０１１３】ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１１４】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図９を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２＝ｃｈ　ｍｏｄ　ｒを計算する。

【０１１５】ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図８のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ　ｍｏｄ　ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１１６】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１１７】ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ　ｍｏｄ　ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１１８】ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成

25

したのではないことがわかる。

【０１１９】本発明の情報取り引きシステムにおいて使用されるコンテンツ利用権識別カードは、コンテンツ利用権管理センタ７００、あるいはコンテンツプロバイダ８００において、電子署名を作成し、コンテンツ利用権管理センタにおいて、電子署名の検証を行なう。コンテンツプロバイダ８００において電子署名を作成し、コンテンツ利用権管理センタ７００において、電子署名の検証を行なう場合は、コンテンツ利用権管理センタ７００は、電子署名の作成を行なったコンテンツプロバイダ８００に対応する電子署名検証用の鍵を保持する構成とする。

【０１２０】図６に戻って、コンテンツ利用権配布手続きについての説明を続ける。図６におけるユーザ端末９００は、コンテンツを取得するとともに、あるいは別ルートで購入したコンテンツ利用権識別カードに記録された識別データを通信手段６００を介してコンテンツ利用権管理センタ７００に送信する。コンテンツ利用権管理センタ７００は、ユーザ端末９００から送信されてきたコンテンツ利用権識別カードのデータについて、署名検証を例えば上述の手法に従って実行してデータの改竄チェックを実行する。

【０１２１】コンテンツ利用権管理センタ７００は、署名検証によりデータ改竄がないことを検証した後、ユーザから送信された識別データ中のコンテンツＩＤとシリアル番号に一致するデータ（図５参照）をデータベース７０４から抽出する。ここで対応するデータの販売回数が０であれば、そのシリアル番号に対応するコンテンツ利用権識別カードに関してはまだ利用権（コンテンツ鍵）の配布を一度も行なっていない、すなわち初回の配布であることが確認され、コンテンツ鍵をコンテンツ鍵格納メモリ７０５から取り出してユーザに対して送信する。なお、コンテンツ鍵は、暗号化して送信することが好ましい。ユーザに対するコンテンツ鍵の送信とともに、データベース７０４の対応データの販売回数を「１」に設定する。

【０１２２】なお、コンテンツ利用権管理センタ７００からユーザ端末９００に対するコンテンツ鍵送信は、ネットワークを介した通信における安全性を考慮して前述したようにコンテンツ鍵を暗号処理部７０２において暗号化処理した後、送信することが望ましい。コンテンツ鍵の暗号化には、共通鍵暗号方式による共通鍵を使用した暗号化処理、あるいは公開鍵暗号方式によるコンテンツ利用権管理センタの秘密鍵による暗号化処理、あるいは、ユーザ端末９００と、コンテンツ利用権管理センタ７００との相互認証処理を実行して生成するセッション鍵を用いて暗号化処理する方法等がある。相互認証処理について、以下、説明する。

【０１２３】共通鍵暗号方式を用いた相互認証方法を、図１０を用いて説明する。図１０において、共通鍵暗号方式としてＤＥＳを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図１０において、Ａ，Ｂは一方が図６におけるユーザ端末９００に対応し、他方がコンテンツ利用権管理センタ７００に対応する。

26

【０１２４】まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。図７に示すＤＥＳのＣＢＣモード処理構成によれば、ＲａがＭ１、ＲｂがＭ２、ＩＤ（ｂ）がＭ３に相当し、初期値：ＩＶ＝０としたときの出力Ｅ１、Ｅ２、Ｅ３が暗号文となる。

【０１２５】これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１２６】次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１２７】これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１２８】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１２９】次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１１を用いて説明する。図１１において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１１において、まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイン

27

トＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。電子署名の生成方法は図８で説明したので、その詳細は省略する。

【０１３０】公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【０１３１】図１２に示す公開鍵証明書の例を示す。図１２に示すように公開鍵証明書には、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【０１３２】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図８で説明した処理フローが適用される。

【０１３３】認証局は、図１２に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【０１３４】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図９で説明したのでその詳細は省略する。

【０１３５】図１１に戻って説明を続ける。Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証方法は図９で説明したので、その詳細は省略する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

28

【０１３６】次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１３７】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ｂｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１３８】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１３９】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１４０】コンテンツ利用権管理センタ７００は、このような相互認証処理において、生成したセッション鍵を用いて、コンテンツ鍵を暗号化して、ユーザ端末９００に対して送信する。

【０１４１】暗号化されたコンテンツ鍵を受信したユーザ端末９００は、暗号処理部３０２において、認証処理の際に生成したセッション鍵を用いてコンテンツ鍵の復号処理を実行する。復号処理によって得られるコンテンツ鍵は、コンテンツ利用権識別カードに記録されたコンテンツ、すなわちメディア５００または通信手段６００を介して受領した暗号化コンテンツを復号可能なコンテンツ鍵であり、ユーザは、このコンテンツ鍵を利用して暗号化コンテンツの復号処理を実行し、コンテンツを利用可能なデータに復号する。

【０１４２】このように、本発明の情報取り引きシステムおよび情報取り引き方法に従えば、コンテンツプロバイダ、コンテンツ販売会社等は、クレジットカード、あるいは銀行口座指定によるオンラインでの決済システムを構築する必要がなく、コンテンツの利用料金をコンテンツ利用権識別カードの販売料金としてコンテンツ利用

権識別カードの流通ルートを介して回収することが可能となる。従って、クレジットカード、または銀行口座を持たないユーザによるコンテンツの利用が容易になる。

【０１４３】なお、上述した説明においては、コンテンツプロバイダがコンテンツの作成、配信を一括して行なう構成として説明したが、コンテンツの作成をコンテンツプロバイダが実行して、コンテンツプロバイダの作成したコンテンツの暗号化処理、配信サービスをコンテンツプロバイダからコンテンツの提供を受けたサービスプロバイダが実行する構成としてもよい。

【０１４４】［コンテンツ利用権の再販］上述した例では、コンテンツ利用権識別カードに基づくコンテンツ鍵の配布は１回のみ行われる構成であったが、本発明の情報取り引きシステムおよび情報取り引き方法におけるコンテンツ利用権識別カードを用いることにより、コンテンツ利用権識別カードを取得したユーザか他のユーザに同一のコンテンツ利用権識別カードを譲渡することにより、コンテンツ利用権識別カードを譲渡された他のユーザが、そのコンテンツ利用権識別カードに基づいてコンテンツ鍵をコンテンツ利用権管理センタから新たに取得する構成が実現される。以下、この構成について説明する。

【０１４５】図１３にコンテンツ利用権識別カードをユーザ間において譲渡し、異なるユーザが同一のコンテンツ利用権識別カードに基づいてコンテンツ鍵を取得する構成を説明する図を示す。図１３においてユーザ（ユーザ端末）１３０１はコンテンツプロバイダ１３０３から暗号化コンテンツを取得し、コンテンツ利用権識別カードを購入する（図の（１）で示す手続き）。

【０１４６】ユーザ（ユーザ端末）１３０１は、前述した手続きに従って、コンテンツ利用権識別カードの識別データをコンテンツ利用権管理センタ１３０４に送信（図の（２）で示す手続き）し、コンテンツ鍵を受領（図の（３）で示す手続き）してコンテンツを復号してコンテンツの利用を行なう。ユーザ（ユーザ端末）１３０１は、暗号化コンテンツの格納されたメディアとコンテンツ利用権識別カードをユーザ（ユーザ端末）１３０２に譲渡（図の（４）で示す手続き）する。

【０１４７】ユーザ（ユーザ端末）１３０２は、譲渡されたコンテンツ利用権識別カードの識別データをコンテンツ利用権管理センタ１３０４に送信（図の（５）で示す手続き）し、コンテンツ鍵を受領（図の（６）で示す手続き）してコンテンツを復号してコンテンツの利用を行なう。

【０１４８】なお、この場合のコンテンツ利用料金のユーザ（ユーザ端末）１３０２からの回収は、従来のクレジットカード、銀行口座指定による料金回収が可能である。あるいは、コンテンツ利用権識別カードに設定した再販可能回数に応じたコンテンツ利用権識別カード価格を設定して最初のユーザに販売するようにしてもよい。例えば再販不可能なコンテンツ利用権識別カード、すなわちは１つのコンテンツ鍵の取得が可能なコンテンツ利用権識別カードが１０００円としたとき、1回再販可能なコンテンツ利用権識別カード、すなわち初回を合わせて2回、コンテンツ鍵を取得可能なコンテンツ利用権識別カードを２０００円、２回再販可能なコンテンツ利用権識別カード、すなわち初回を合わせて３回、コンテンツ鍵を取得可能なコンテンツ利用権識別カードを３０００円で販売する設定とすれば、コンテンツ利用権識別カードを譲渡されたユーザもオンライン決済手続き等が不要となる。なお、２回、３回等の複数回のコンテンツ鍵取得権を有するカードについては割り引きを行なって販売する構成としてもよい。

【０１４９】コンテンツ利用権管理センタ１３０４は、このようなコンテンツ利用権識別カードの再販可能情報は、先に図５を用いて説明したコンテンツ利用権管理センタデータベースにおいて管理している。図５から理解されるように発行されたコンテンツ利用権識別カードはシリアル番号が付与され、個々のカードが識別可能であり、それらについて再販可能性、最大可能回数Ｎが設定されている。図５の例では、上段の２つのコンテンツ利用権識別カードは再販ができない、すなわち1回限りコンテンツ鍵を取得可能なコンテンツ利用権識別カードである。中段の２つのコンテンツ利用権識別カードは、再販が可能なコンテンツ利用権識別カードであり、再販回数が規定されていないカードである。下段の２つのカードは、再販回数がＮに設定されており、Ｎ回までコンテンツ鍵をコンテンツ利用権管理センタ１３０４から取得可能な鍵として設定されている。

【０１５０】コンテンツ利用権管理センタ１３０４は、ユーザからコンテンツ利用権識別カードデータを受信した際、図５に示すデータベース中の対応データを抽出して、その設定情報に従って、コンテンツ鍵の送信、非送信を決定する。例えばＮ回までコンテンツ鍵をコンテンツ利用権管理センタ１３０４から取得可能な鍵として設定されたコンテンツ利用権識別カードデータの受信を受けた場合には、販売回数をチェックし、Ｎを超えない範囲においてのみコンテンツ鍵を送信する。コンテンツ利用権管理センタ１３０４がコンテンツ鍵の送信を行なった場合は、データベースの販売回数を1インクリメントする。

【０１５１】また、図５に示すデータ中には、購入者情報が記録されており、コンテンツ利用権管理センタ１３０４は、最初にコンテンツ利用権識別カードを購入したユーザ情報を、そのコンテンツ利用権識別カードのシリアル番号に対応付けて登録し、そのコンテンツ利用権識別カードに基づく複数回のコンテンツ購入依頼があった場合に、購入回数に応じたポイントを登録ユーザに付与して、例えば異なるコンテンツ購入、あるいはコンテンツ利用権識別カード購入料金をポイントに応じて割り引

くサービスを提供する。

【０１５２】なお、コンテンツ利用権識別カードに付与されるシリアル番号は、流通経路毎に分類する構成とすることが好ましい。この構成とすることにより、シリアル番号に基づいて、その流通経路が判別可能となり、コンテンツ利用権識別カードの改竄等により不正なシリアル番号を持つコンテンツ利用権識別カードが市場に流通することを防止することができる。

【０１５３】さらに、コンテンツ利用権管理センタ１３０４は、管理データとして、ユーザの同一性判定情報、ユーザ機器の機器情報を持つことにより、同一ユーザからの利用の場合にポイントを付与したり、また、同一機器からのコンテンツ鍵取得要求には、繰り返し応じる等の処理が可能となる。

【０１５４】このデータベース例を図１４に示す。図１４に示すデータベースには、利用対象となるコンテンツを識別するコンテンツ識別子（ＩＤ）と、シリアル番号、利用権（復号鍵）の販売回数、利用権の購入者情報、ユーザ識別データ、ユーザ機器識別データ、その他の情報が含まれる。コンテンツ識別子（ＩＤ）と、シリアル番号、利用権（復号鍵）の販売回数、利用権の購入者情報、その他の情報は、前述の図５において説明したと同様のデータである。

【０１５５】ユーザ識別データは、コンテンツ利用権識別カードデータを送信したユーザから取得する、例えばユーザＩＤ＋パスワード、あるいは指紋、虹彩、声紋等、ユーザ固有のバイオメトリックス情報を登録しておき、これらの情報をコンテンツ利用権管理センタ１３０４がユーザからのコンテンツ利用権識別カードデータ受信に際して受信してユーザ同一性を判定し、同一ユーザの利用であった場合には、ユーザに対するポイントを付与する。

【０１５６】また、ユーザ機器識別データは、ユーザの使用機器のＩＤを登録して、同一ユーザ機器からのコンテンツ鍵取得要請であった場合には、コンテンツ鍵の繰り返し送信を許容する構成とすることができる。なお、ユーザ使用機器の同一性判定は、前述の図１０、１１の相互認証処理において実行可能である。

【０１５７】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１５８】

【発明の効果】上述したように、本発明の情報取り引きシステムおよび情報取り引き方法に従えば、コンテンツプロバイダ、コンテンツ販売会社等は、クレジットカード、あるいは銀行口座指定によるオンラインでの決済システムを構築する必要がなく、また、ユーザ間において同一のコンテンツ利用権識別カードの譲渡が可能となり、同一の識別に基づいて複数回コンテンツ鍵を送受信することが可能となり、コンテンツの利用が促進される。コンテンツプロバイダ、コンテンツ販売会社等は、コンテンツの利用料金をコンテンツ利用権識別カードの販売料金としてコンテンツ利用権識別カードの流通ルートを介して回収することが可能となる。従って、クレジットカード、または銀行口座を持たないユーザによるコンテンツの利用が容易になる。

【図面の簡単な説明】

【図１】従来の暗号化コンテンツ利用形態を説明する図である。

【図２】本発明の情報取り引きシステムにおいて利用可能なデータ処理装置の構成を示す図である。

【図３】本発明の情報取り引きシステムにおけるコンテンツ、コンテンツ利用権識別カードの流通形態を説明する図である。

【図４】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードのデータ構成を示す図である。

【図５】本発明の情報取り引きシステムにおけるコンテンツ利用権管理センタのデータベースのデータ構成を示す図である。

【図６】本発明の情報取り引きシステムにおけるユーザ端末、コンテンツ利用権管理センタ、コンテンツプロバイダの構成を説明する図である。

【図７】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名生成について説明する図である。

【図８】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名生成について説明する図である。

【図９】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名検証について説明する図である。

【図１０】本発明の情報取り引きシステムにおける相互認証処理について説明する図である。

【図１１】本発明の情報取り引きシステムにおける相互認証処理について説明する図である。

【図１２】本発明の情報取り引きシステムにおける相互認証処理において使用される公開鍵証明書の構成について説明する図である。

【図１３】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの再販構成を説明する図である。

【図１４】本発明の情報取り引きシステムにおけるコンテンツ利用権管理センタのデータベースのデータ構成を示す図である。

【符号の説明】

１０６　メインＣＰＵ

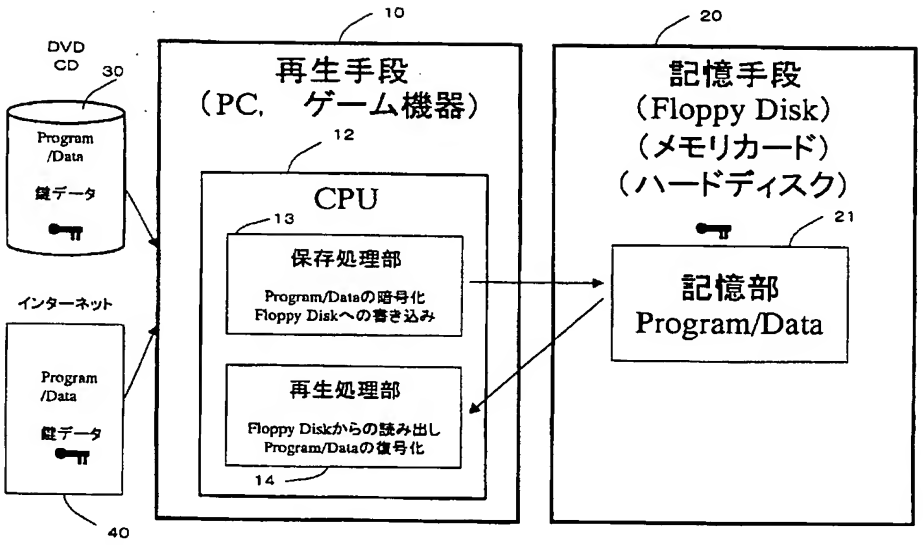
33

１０７　ＲＡＭ
１０８　ＲＯＭ
１０９　ＡＶ処理部
１１０　入力処理部
１１１　ＰＩＯ
１１２　ＳＩＯ
３００　記録再生器
３０１　制御部
３０２　暗号処理部
３０３　記録デバイスコントローラ
３０４　読み取り部
３０５　通信部
３０６　制御部
３０７　内部メモリ
３０８　暗号／復号化部
４００　記録デバイス
４０１　暗号処理部
４０２　外部メモリ
５００　メディア

34

５５０　通信手段
６０１　ユーザ端末
６０２，６０３，６０４　コンテンツプロバイダ
６０５　コンテンツ利用権管理センタ
６０６　メディア
６０７　ネットワーク
７００　コンテンツ利用権管理センタ
７０１　制御部
７０２　暗号処理部
７０３　通信部
７０４　データベース
７０５　コンテンツ鍵格納メモリ
８００　コンテンツプロバイダ
８０１　制御部
８０２　暗号処理部
８０３　通信部
８０４　データベース
９００　ユーザ端末

【図１】

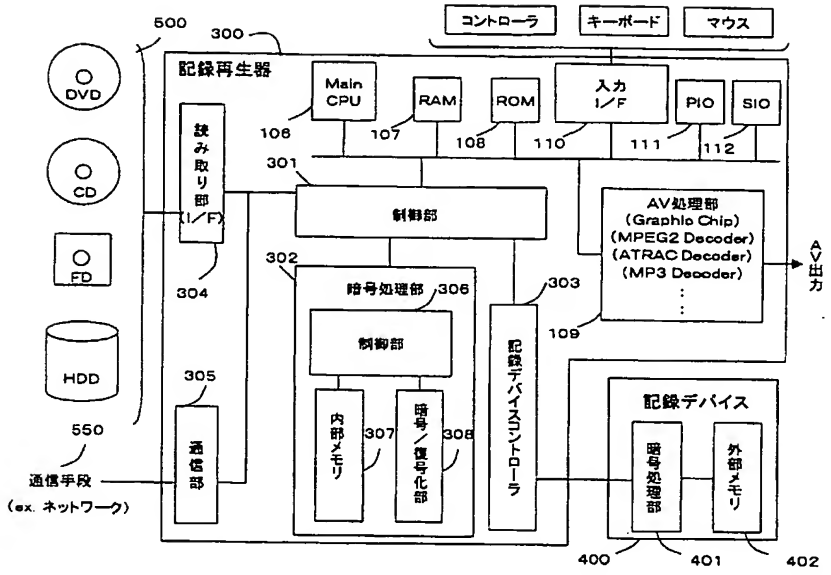


【図４】

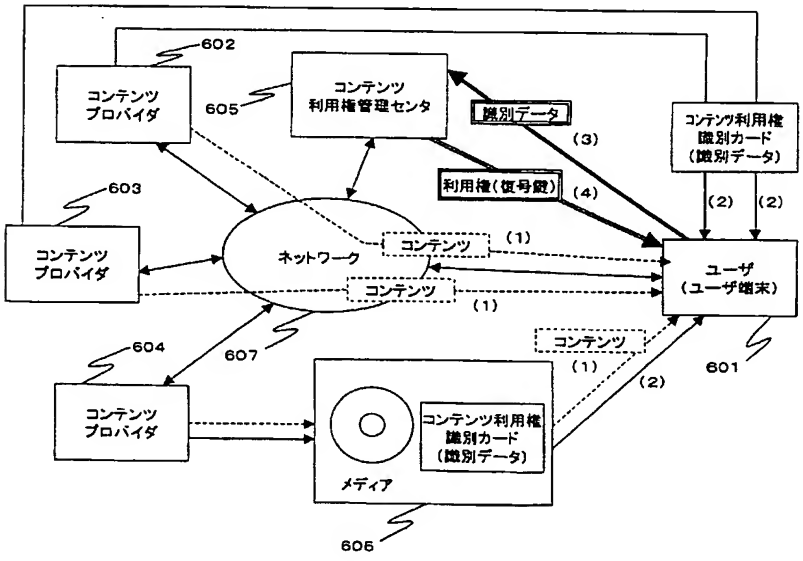
識別データ構成

コンテンツID	シリアル番号	電子署名
01234567	0000123	34251748

【図２】


コントローラ
キーボード
マウス
500
300
記録再生器
DVD
CD
FD
HDD
Main CPU
RAM
ROM
入力 I/F
PIO
SIO
106
107
108
110
111
112
読み取り部 (I/F)
304
301
制御部
AV処理部 (Graphic Chip) (MPEG2 Decoder) (ATRAC Decoder) (MP3 Decoder)
出力
302
暗号処理部
306
制御部
内部メモリ
307
暗号／復号化部
308
303
記録デバイスコントローラ
109
305
通信部
550
通信手段
(ex. ネットワーク)
記録デバイス
暗号処理部
外部メモリ
400
401
402

【図３】

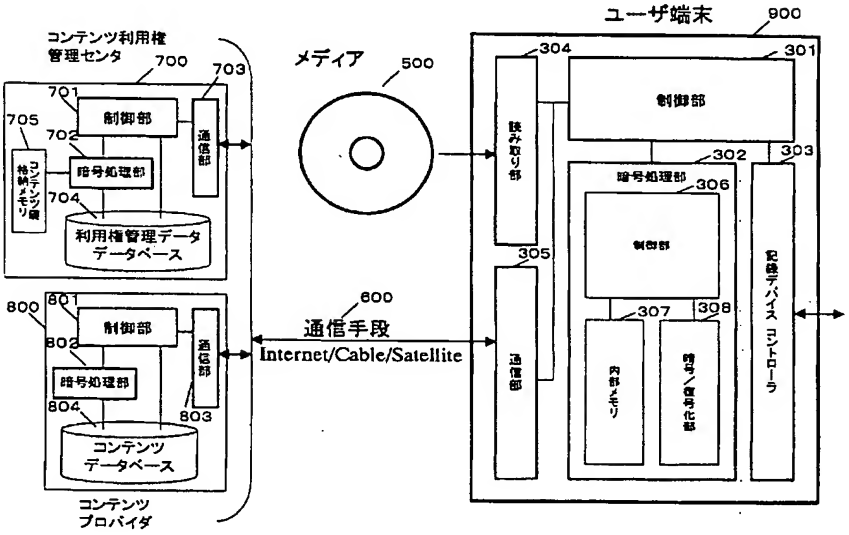

602
コンテンツ プロバイダ
605
コンテンツ 利用権管理センタ
識別データ
(3)
コンテンツ利用権 識別カード (識別データ)
利用権(復号鍵)
(4)
(2)
(2)
603
コンテンツ プロバイダ
ネットワーク
コンテンツ
(1)
ユーザ (ユーザ端末)
コンテンツ
(1)
604
607
コンテンツ
(1)
(2)
601
コンテンツ プロバイダ
コンテンツ利用権 識別カード (識別データ)
メディア
606

【図５】

コンテンツ利用権管理センタデータベース

コンテンツID	シリアル番号	販売回数	購入者情報	その他
01234567	0000123	0		再販不可能
01234567	0000124	0		再販不可能
99999999	0000125	1	ACD22222	再販可能
99999999	0000126	2	BBF33333	再販可能
22222222	0000127	5		最大販売回数N
22222222	0000128	N−1		最大販売回数N

【図６】

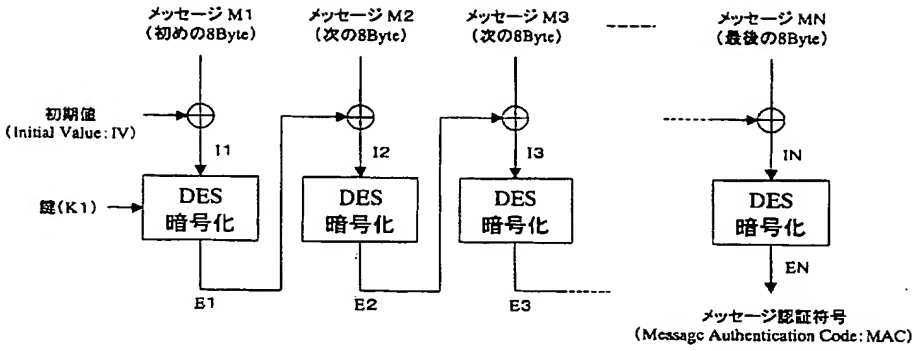


【図１４】

コンテンツ利用権管理センタデータベース

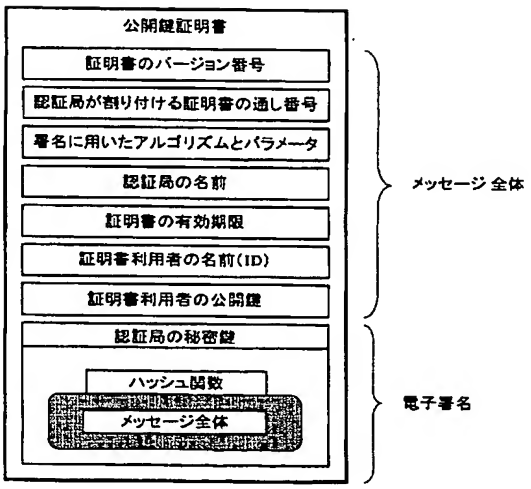
コンテンツID	シリアル番号	販売回数	購入者情報	ユーザ識別データ	ユーザ機器識別データ	その他
01234567	0000123	0				再販不可能
01234567	0000124	0				再販不可能
99999999	0000125	1	ACD22222	BCD38432	ABA23255	再販可能
99999999	0000126	2	BBF33333	BBB28756	BBC37854	再販可能
22222222	0000127	5	CBD36578	CDA15683	BBA36529	最大販売回数N
22222222	0000128	N−1	BDD28215	ABB19653	CBB35532	最大販売回数N

【図７】



⊕ ：排他的論理和処理(8バイト単位)

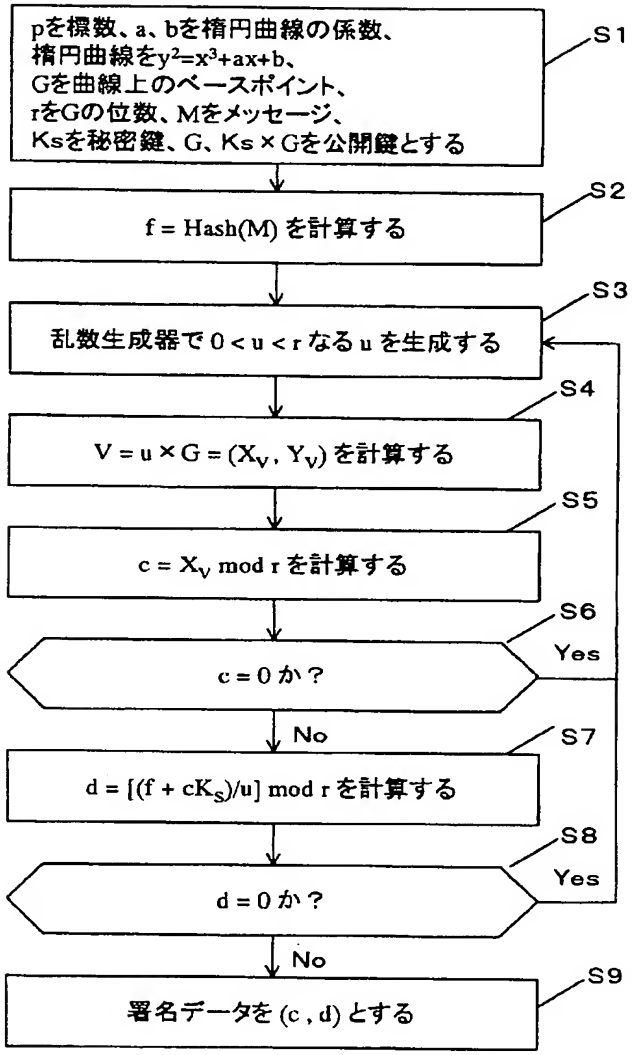
【図１２】



公開鍵証明書

【図８】

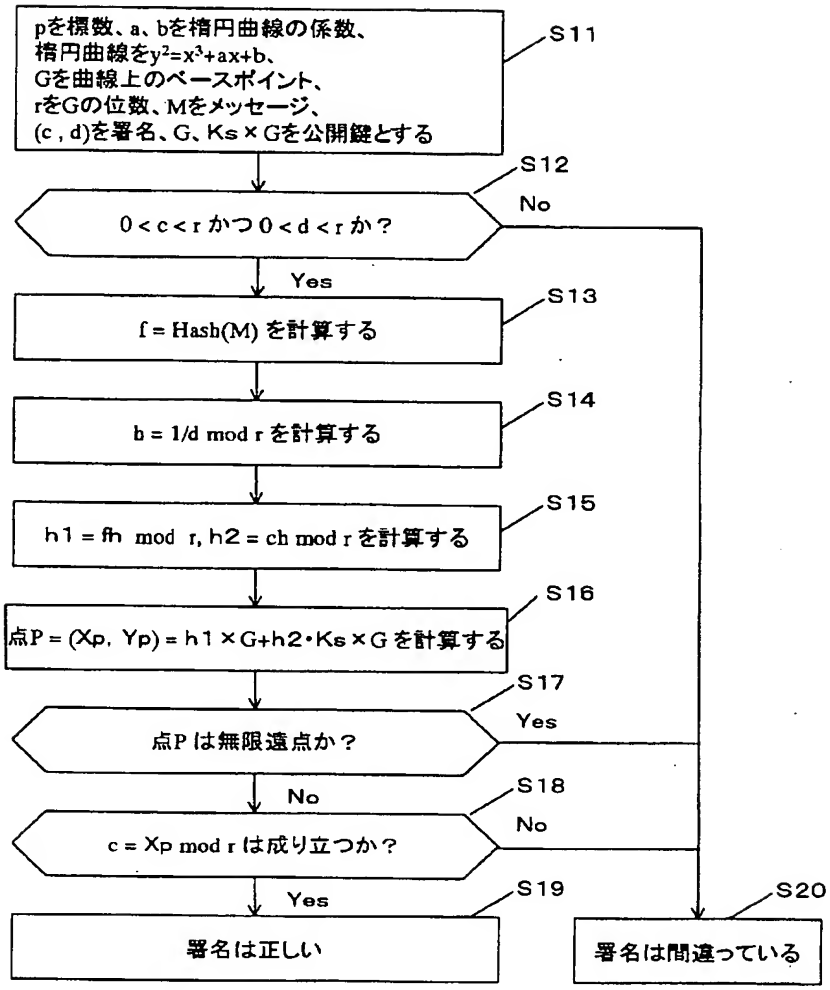
署名生成



署名生成（IEEE P1363/D3）

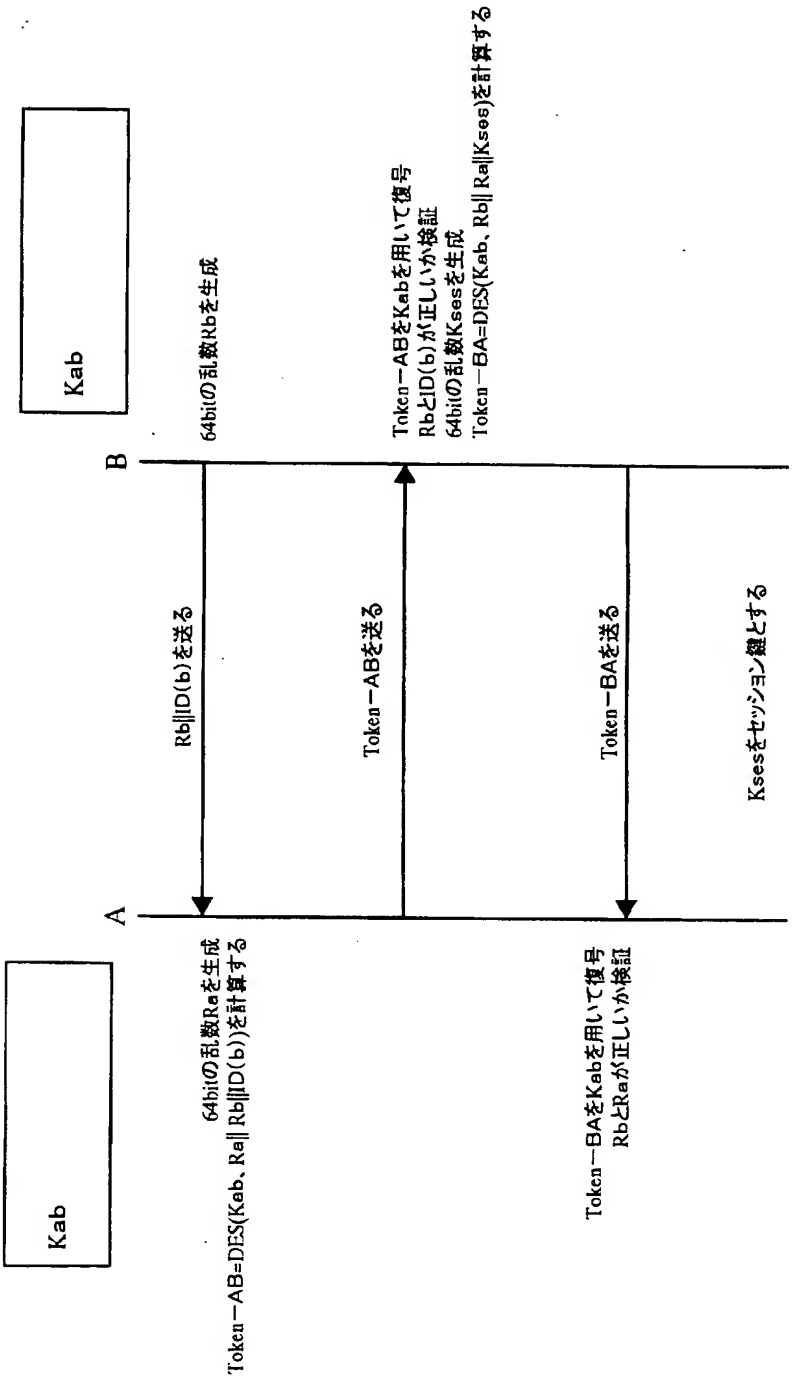
【図９】

署名検証



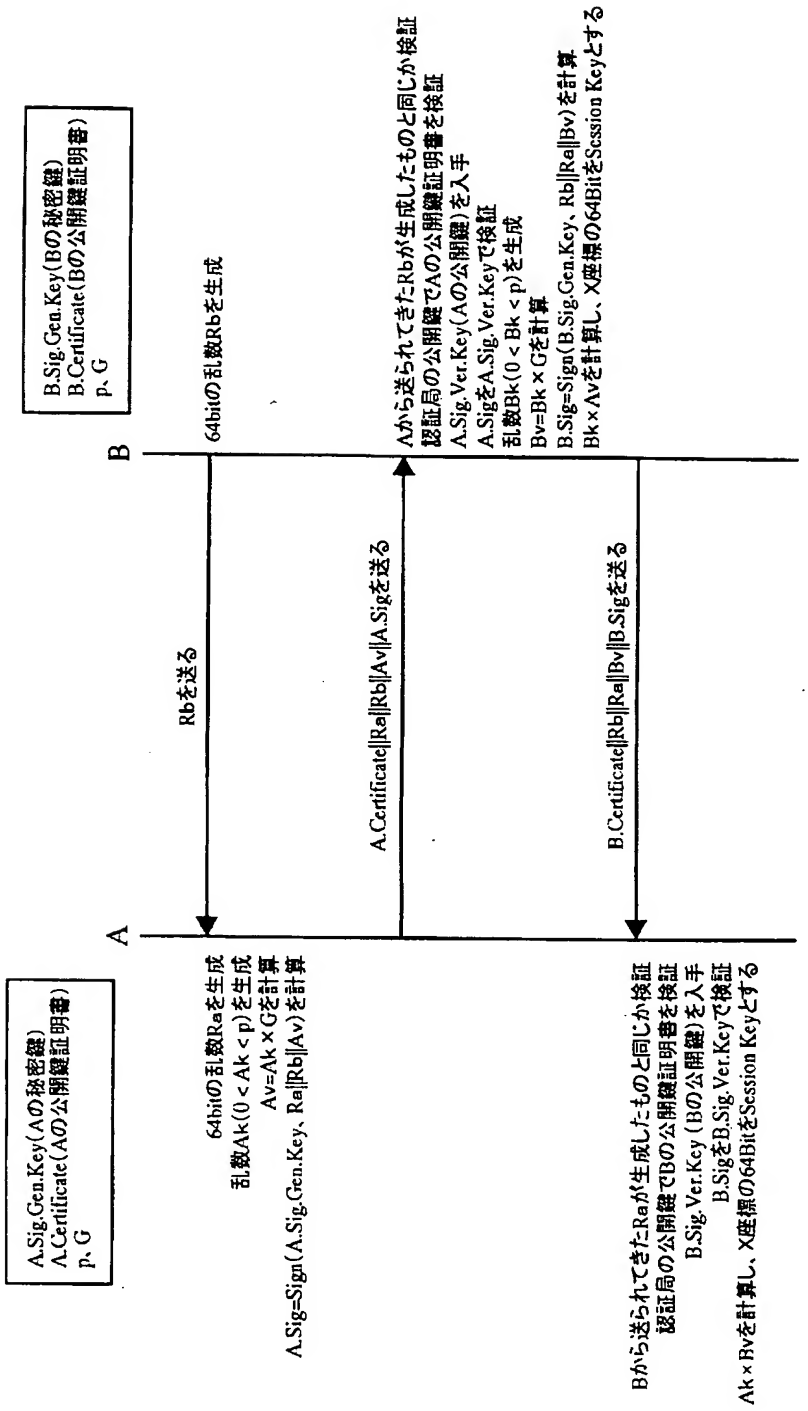
署名検証(IEEE P1363/D3)

【図１０】



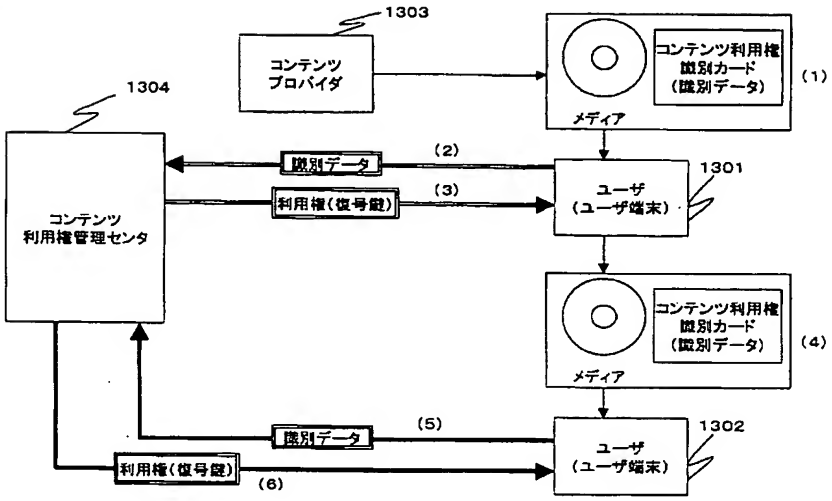
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１１】



ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１３】



フロントページの続き

(51) Int. Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０７Ｆ	7/08		Ｇ０９Ｃ	1/00	６４０Ｂ　９Ａ００１
	17/00		Ｈ０４Ｌ	9/00	６０１Ｂ
Ｇ０９Ｃ	1/00	６２０	Ｇ０６Ｆ	15/21	ＺＥＣＺ
		６４０			３４０Ｚ
			Ｇ０７Ｆ	7/08	Ｒ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ

Ｆターム(参考)　3E044 BA04 DA05 DC05 DC06 DD02
DE01
5B017 AA06 BA07 CA15 CA16
5B049 AA05 BB11 CC08 CC36 DD01
DD04 DD05 EE03 EE07 EE21
FF06 FF08 FF09 GG02 GG04
GG07 GG10
5B085 AE12 AE13 AE23 AE29
5J104 AA09 AA16 EA16 JA13 JA14
JA25 JA28 LA02 LA03 LA06
MA06 NA02 NA12 NA33 NA37
PA07 PA14
9A001 CZ02 EE03 FF01 JZ76 KK60
KK62 LL03